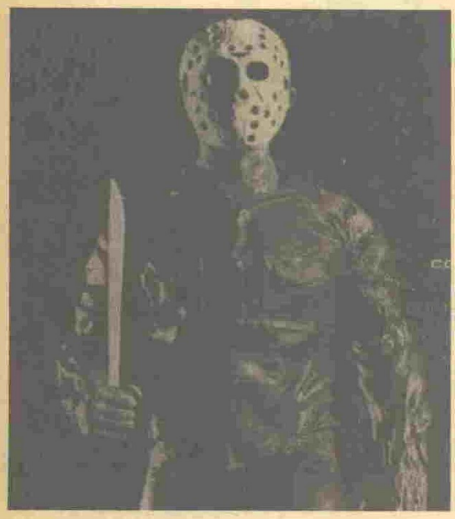
FRIDAY

โปรแกรมพิฆาตไวรัสศุกร์ที่ 13

ภูษิต สระปัญญา

เรื่องไวรัสคอมพิวเตอร์เป็นเรื่องที่ได้รับความสนใจอยู่มาก ในประเทศไทยเองนั้นก็มีไวรัสระบาดอยู่หลายชนิด ซึ่งนักเขียนโปรแกรมก็ได้เขียนโปรแกรมกำจัดไวรัสกันมากมาย รวมถึงการสร้างอุปกรณ์ทางฮาร์ดแวร์เพื่อป้องกันและกำจัดไวรัส ไวรัสเหล่านั้นจะซ่อนตัวอยู่ในบูตเซกเตอร์ (เซกเตอร์ที่บรรจุโปรแกรมเพื่อทำงานเมื่อมีการบูตหรือรีเซต) ซึ่งสามารถแก้ไขได้โดยนำบูตเซกเตอร์ของดิสเกตต์แผ่นที่ไม่ติดไวรัสมาเขียนทับในบูตเซกเตอร์ของแผ่นที่ติดไวรัส หลังจากนั้นก็ใช้โปรแกรมยูทิลิตี้เช่น PCTOOLS มาแก้ไขผลข้างเคียงที่เกิดจากการกระทำของไวรัส เช่น การเปลี่ยนชื่อดิสเกตต์ การทำลายไฟล์ การทำลายบางเซกเตอร์ เป็นต้น ส่วนการทำงานของไวรัสจะเริ่มต้นเมื่อมีการบูต (ด้วยปุ่ม Ctrl + Alt + Del) ตัวไวรัสก็จะเข้าไปฝังตัวในหน่วยความจำ พร้อมกับเปลี่ยนอินเตอร์รัพต์เวกเตอร์บางตัวให้มาทำงานเป็นไวรัส (อินเตอร์รัพต์คือการร้องขอให้เครื่องคอมพิวเตอร์ทำงานต่าง ๆ ในระดับย่อยที่สุด โดยผู้ใช้หรืออุปกรณ์อื่น ๆ ซึ่งจะมีโปรแกรมอินเตอร์รัพต์นี้อยู่เรียบร้อยแล้วเมื่อทำการเปิดเครื่องคอมพิวเตอร์ แล้วบูตด้วยแผ่นดิสเกตต์ที่มีระบบจัดการอยู่ และอินเตอร์รัพต์เวกเตอร์คือตัวที่ชี้ที่อยู่ของโปรแกรมอินเตอร์รัพต์) วิธีแก้ง่าย ๆ คือรีเซตเครื่องใหม่ หรือวิธียากขึ้นมาอีกคือเปลี่ยนอินเตอร์รัพต์เวกเตอร์ให้ชี้ในตำแหน่งที่ถูกต้อง แต่วิธีนี้จะต้องรู้รายละเอียดของไวรัสแต่ละชนิด ซึ่งผู้เขียนได้ใช้วิธีนี้ในโปรแกรมกำจัดไวรัสที่จะกล่าวถึงต่อไป

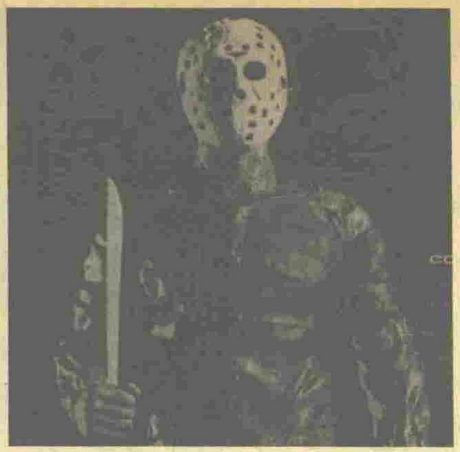


ผู้เขียนได้พบไวรัสชนิดหนึ่งซึ่งน่าสนใจมาก โดยไวรัสจะซ่อนตัวอยู่ในไฟล์ที่สามารถรันได้ในระบบจัดการโดยตรง (นามสกุล .COM หรือ .EXE) แทนที่จะอยู่ในบูตเซกเตอร์ ทำให้สังเกตได้ยาก เนื่องจากไวรัสชนิดนี้ไม่มีชื่อแสดงไว้ผู้เขียนจะขอเรียกว่าศุกร์ที่ 13 (FRIDAY 13th) (ไวรัสนี้มีชื่อที่มีผู้เรียกใช้กันมากคือ "อิสราเอล") ผู้เขียนได้แยกตัวโปรแกรมของศุกร์ที่ 13 ออกจากโปรแกรมที่ติดไวรัสนี้เพื่อศึกษารายละเอียดพร้อมกับได้เขียนโปรแกรม (ภาษาแอสเซมบลี) เพื่อทำลายศุกร์ที่ 13 ทั้งในหน่วยความจำและดิสเกตต์ โดยจะแสดงรายละเอียดต่อไป

ลักษณะของศุกร์ที่ 13

1. มีขนาด 1813 ไบต์ในไฟล์นามสกุล .COM และ 1808 ไบต์ในไฟล์นามสกุล .EXE

2. ซ่อนตัวอยู่ต้นโปรแกรมของไฟล์นามสกุล .COM (ติดไวรัสได้เพียง 1 ครั้ง นั่นคือโปรแกรมที่ติดไวรัสแล้วจะไม่ติดซ้ำอีกเนื่องจากการจำกัดขนาดของไฟล์นามสกุล .COM) แต่ถ้าซ่อน



ตัวอยู่ในโปรแกรมนามสกุล .EXE จะซ่อนตัวต่อท้ายโปรแกรมและสามารถติดไวรัสได้อีกเรื่อย ๆ และยังไปแก้ FILE HEADER ของไฟล์ด้วย (FILE HEADER คือส่วนหัวที่บอกลักษณะและโครงสร้างของไฟล์นามสกุล .EXE ซึ่งต้องมีในไฟล์นามสกุล .EXE ทุกไฟล์)

3. เมื่อเรียกใช้งานไฟล์ที่มีศุกร์ที่ 13 อยู่ตัวไวรัสจะเข้าไปฝังตัวในหน่วยความจำ พร้อมกับเปลี่ยนอินเตอร์รัพต์เวกเตอร์หมายเลข 21h และอินเตอร์รัพต์เวกเตอร์หมายเลข 8h จะถูกเปลี่ยนด้วยถ้ามีการเรียกไฟล์นามสกุล .COM หรือ .EXE ไฟล์เหล่านั้นก็จะติดไวรัสไป เนื่องจากอินเตอร์รัพต์เวกเตอร์หมายเลข 21h ฟังก์ชัน 4Bh (EXECUTE PROGRAM) ซึ่งถูกใช้งานโดยศุกร์ที่ 13 จะเขียนตัวโปรแกรมไวรัสลงไปในไฟล์ที่ถูกเรียก ทำให้ไฟล์มีขนาดเพิ่มขึ้น

4. เมื่อบูตเครื่องใหม่อินเตอร์รัพต์เวกเตอร์จะกลับไปชี้ที่ตำแหน่งที่ถูกต้อง นั่นหมายความว่าไวรัสในหน่วยความจำจะทำงานไม่ได้แล้ว

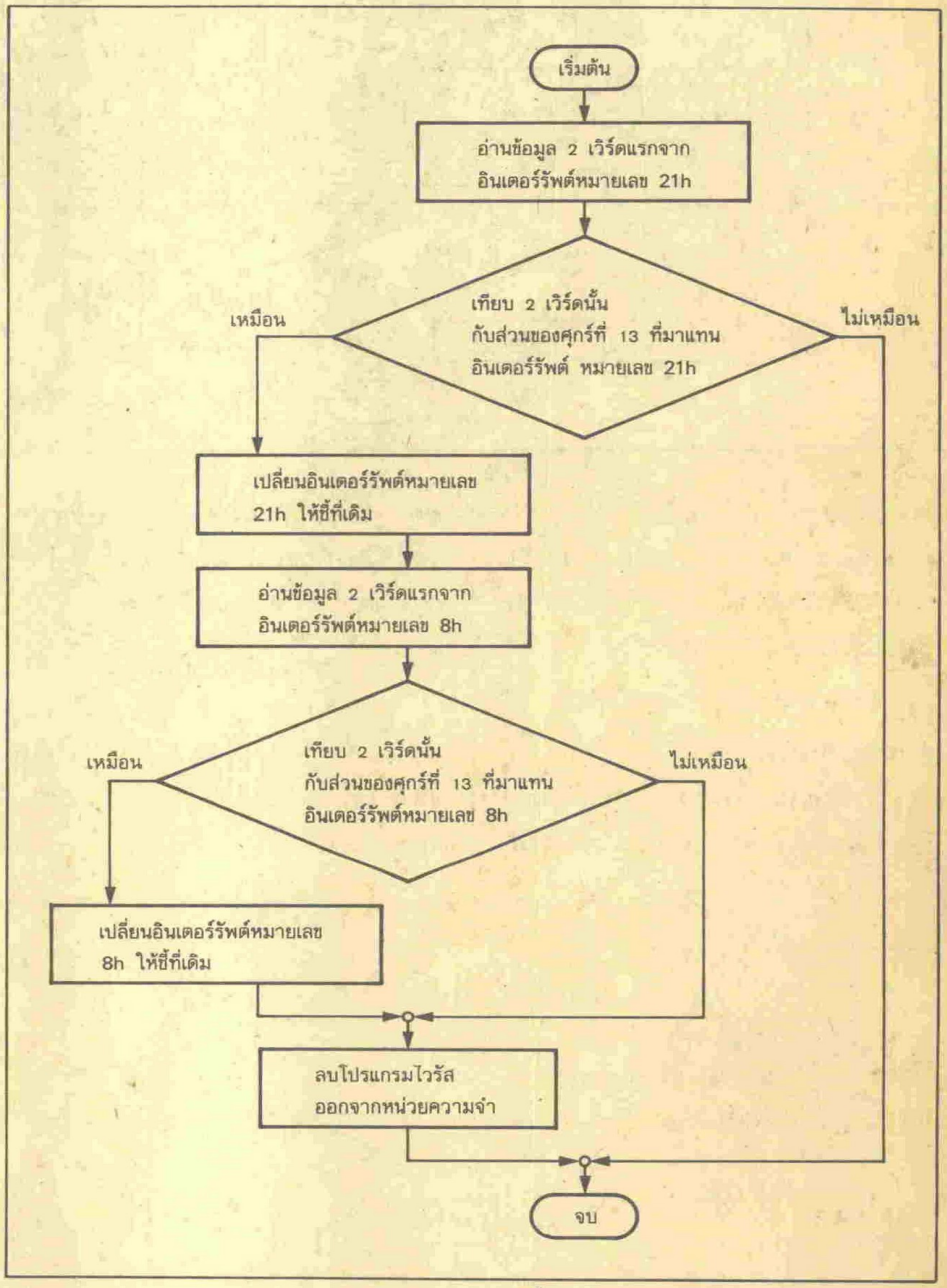
5. ในวันศุกร์ที่ 13 ที่ไม่ใช่ปี ค.ศ. 1987 ถ้ามีการเรียกใช้โปรแกรมที่ติดไวรัสทำให้ไวรัสฝังตัวในหน่วยความจำแล้ว ไม่ว่าจะเรียกใช้โปรแกรมใด โปรแกรมนั้นจะถูกลบทิ้งจากแผ่นดิสเกตต์ทันที นี่เป็นเหตุผลที่ผู้เขียนเรียกไวรัสชนิดนี้ว่าศุกร์ที่ 13 แต่โปรแกรมที่ถูกลบทิ้งอาจกู้กลับมาได้

การทำลายศุกร์ที่ 13 ในหน่วยความจำ

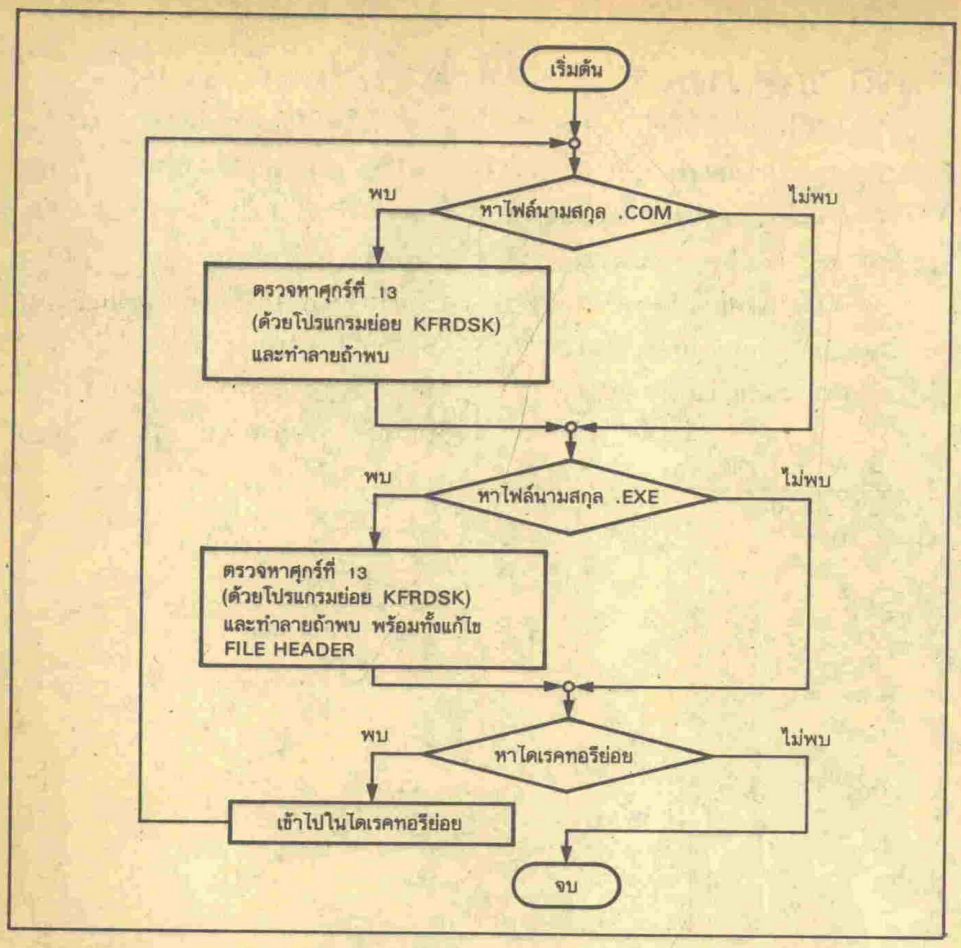
จะใช้โปรแกรมย่อยชื่อ FRMEM (FRIDAY 13th IN MEMORY) ดูขั้นตอนการทำงานของโปรแกรมดูในรูปที่ 1 (ส่วนตัวโปรแกรมทำลายศุกร์ที่ 13 ทั้งหมดได้จัดลงในซอฟต์เมล์ฉบับนี้ เนื่องจากโปรแกรมค่อนข้างยาว จึงไม่สะดวกที่จะจัดลงในบทความได้)

การทำลายศุกร์ที่ 13 ในดิสเกตต์

จะใช้โปรแกรมย่อยชื่อ FRDSK (FRIDAY 13th IN DISKETTE) ดูขั้นตอนการทำงานในรูปที่ 2 จะสามารถทำลายไวรัสได้ในทุกโปรแกรม ไม่ว่าจะอยู่ในไดเรคทอรีใด โดยจะมีการถามชื่อไดรฟ์ก่อนในกรณีที่ผู้อ่านไม่คุ้นเคยกับการค้นหาไฟล์ต่าง ๆ ด้วยการใช้อินเตอร์รัพต์หมายเลข 21h ก็ไม่ต้อง



รูปที่ 1 แผนผังการทำงาน ของโปรแกรมย่อย FRMEM



รูปที่ 2 แผนผังการทำงาน ของโปรแกรมย่อย FRDSK

สนใจกับการค้นหาไฟล์ก็ได้ ส่วนรูปที่ 3 นั้นแสดงแผนผังการทำงานของโปรแกรมย่อย KFRDSK (KILL FRIDAY 13 TH IN DISKETTE)

โปรแกรมภาษาแอสเซมบลี ทำลายศุกร์ที่ 13

โปรแกรมนี้ทำงานโดยตรวจศุกร์ที่ 13 ในหน่วยความจำและไฟล์นามสกุล .COM, .EXE และทำลายไวรัสออกถ้าพบไวรัส (โปรแกรมนี้ใช้มาโครแอสเซมเบลอร์เวอร์ชัน 5.00)

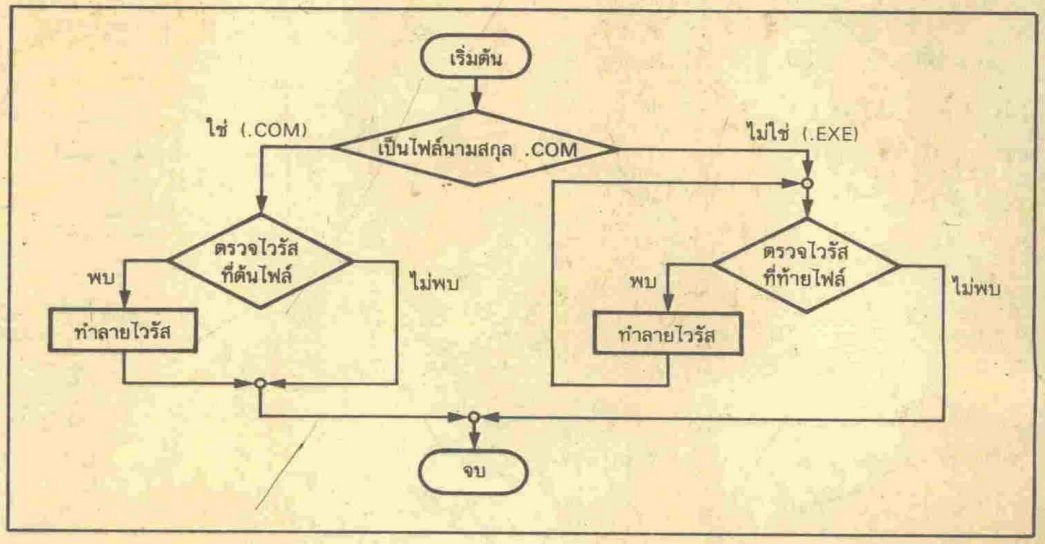
ข้อจำกัดของโปรแกรม

1. ไม่สามารถทำลายไวรัสในไฟล์ขนาดมากกว่า 60,000 ไบต์ได้ เพราะจะทำให้โปรแกรมในช่วงอ่านและเขียนไฟล์สับสนเกินไป (ได้เปิดโอกาสให้เพิ่มเติมแล้วในโปรแกรมที่ตัวแปร FSIZE1 และ FSIZE2 จะเก็บขนาดของไฟล์ทั้งหมดอยู่ แต่ผู้เขียนใช้แต่ขนาดไฟล์ในตัวแปร FSIZE2 เท่านั้น)

2. เมื่อมีข้อผิดพลาดใด ๆ เกิดขึ้น จะแสดงเพียงข้อความ "ERROR!" เท่านั้น ไม่ได้บอกสาเหตุของความผิดพลาด

3. ในการใช้โปรแกรมในฮาร์ดดิสค์ จะใช้เวลามากในการค้นหาไวรัสในทุก ๆ ไฟล์ (ทดลองใช้กับฮาร์ดดิสค์ขนาด 30 เมกะไบต์ มีที่ว่าง 3 เมกะไบต์ และไม่มีไวรัสใช้เวลาประมาณ 10 นาที)

โปรแกรม FRIDAY.COM สามารถขอก๊อบปี้ได้ฟรีที่ชมรมคอมพิวเตอร์ ห้อง 403 ตึกจุลจักรพงษ์ จุฬาลงกรณ์มหาวิทยาลัย ทุกวันเว้นวันอาทิตย์



รูปที่ 3 แผนผังการทำงาน ของโปรแกรมย่อย KFRDSK

วิธีใช้โปรแกรมศุกร์ที่ 13

สมมติมีไฟล์ต่าง ๆ ใน ไดรฟ์ C ดังรูปที่ 4 โดยที่ไฟล์ C:FRIDAY.COM เป็นไฟล์ทำลายไวรัสที่ได้กล่าวมาแล้ว และไฟล์ C:TROJUN1.COM, C:\DIR1\DIR2\NYET.EXE, C:\DIR1\DIR3\TROJUN2.COM เป็นไฟล์ที่ติดไวรัสเมื่อรัน C:TROJUN1.COM ไวรัสศุกร์ที่ 13 จะเข้าไปอยู่ในหน่วยความจำ หลังจากนั้นรัน C:FRIDAY.COM จะได้ผลดังรูปที่ 5

สังเกตว่าไฟล์ C:FRIDAY.COM จะติดไวรัสเมื่อเรียกใช้งาน แต่ไวรัสจะถูกทำลายขณะทำงาน ตอนนี้ไวรัสจะถูกทำลายทั้งในหน่วยความจำและทุกไฟล์ในไดรฟ์ C (ดูรูปที่ 6) ไฟล์ C:TROJUN1.COM และ C:\DIR1\DIR3\TROJUN2.COM จะมีขนาดลดลง 1813 ไบต์ ไฟล์ C:\DIR1\DIR2\NYET.EXE มีขนาดเหลือ 25136 ไบต์ ซึ่งเป็นขนาดที่แท้จริงของไฟล์นี้ จากขนาดเดิม 46832 ไบต์ หมายความว่าไฟล์นี้ติดไวรัสมาทั้งหมด = (46832-25136)/1808 = 12 ครั้ง (ขนาดของไวรัส FRIDAY 13th = 1808 ไบต์ในไฟล์นามสกุล .EXE) ลองสังเกตไฟล์ของคุณดูนะครับว่ามีขนาดใหญ่ขึ้นหรือเปล่า ถ้าใช่ก็ลองใช้โปรแกรมนี้ทำลายไวรัสที่ชื่อศุกร์ที่ 13 นี้ดู ขอเตือนว่าทำให้เสร็จก่อนวันศุกร์ที่ 13 ก็แล้วกัน!

```
Directory of C:\
COMMAND    COM      23210    3-07-85   1:43p
MASM       EXE     103175    7-31-87
LINK       EXE      64982    7-31-87
EXE2BIN    EXE       1664   10-20-83  12:00p
FRIDAY     COM       3165    3-26-89  11:14p
TROJUN1    COM       1815    1-01-08  12:03a
DIR1             <DIR>       3-27-89   9:20p
Directory of C:\DIR1\DIR2
.                <DIR>       3-27-89   9:20p
..               <DIR>       3-27-89   9:20p
NYET       EXE      46832    7-01-88   6:17p
Directory of C:\DIR1\DIR3
.                <DIR>       3-27-89   9:20p
..               <DIR>       3-27-89   9:20p
TROJUN2    COM       1815    1-01-80  12:03a
```

รูปที่ 4

```
=========VIRUS ENEMY=========
Checking memory...
  Have FRIDAY 13th in memory, I had kill it !
Check drive ? C
Checking drive:C...
  Have Friday 13th in file...
    C:\FRIDAY.COM, I had kill it !
    C:\TROJUN1.COM, I had kill it !
    C:\DIR1\DIR2\TROJUN2.COM, I had kill it !
    C:\DIR1\DIR2\NYET.EXE, I had kill it !
Check another diskette (y/n) ? N
```

รูปที่ 5

```
Directory of C:\
COMMAND    COM      23210    3-07-85   1:43p
MASM       EXE     103175    7-31-87
LINK       EXE      64982    7-31-87
EXE2BIN    EXE       1664   10-20-83  12:00p
FRIDAY     COM       3165    3-27-89   9:22p
TROJUN1    COM          2    3-27-89   9:22a
DIR1             <DIR>       3-27-89   9:20p
Directory of C:\DIR1\DIR2
.                <DIR>       3-27-89   9:20p
..               <DIR>       3-27-89   9:20p
NYET       EXE      25136    3-27-89   9:23p
Directory of C:\DIR1\DIR3
.                <DIR>       3-27-89   9:20p
..               <DIR>       3-27-89   9:20p
TROJUN2    COM          2    3-27-89   9:22p
```

รูปที่ 6